



NEMZETI KIBERVÉDELMI INTÉZET

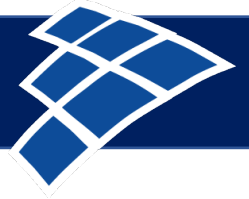


A Nemzeti Kibervédelmi Intézet (NKI) feladatai - érdekes esetek a közelmúltból

Marsi Tamás
2022. – Debrecen EIVOK



NKI felépítése



Nemzetbiztonsági Szakszolgálat



Nemzeti Kibervédelmi Intézet

CSIRT



- Incidenskezelés
- Riasztás
- Tájékoztatás

Biztonsági elemzés



- Log-elemzés
- Forensics
- Malware elemzés

Esemény-észlelés



- EWS
- Honeypot
- Big data
- Trend-elemzés

Pentest



- Külső
- Belső
- Webes
- Wifi
- Social engineering

SOC



- Biztonság-irányítás
- Biztonság-felügyelet
- EMIR/ FAIR /IMIR

Hatóság



- Nyilvántartás
- Ellenőrzés
- SPOC

- Kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelem biztosítása
- Támadás megszakítás
- Adatellenőrzés
- Koordináció
- Tudatosítás
- Média



Megfelelőség (hatóság)



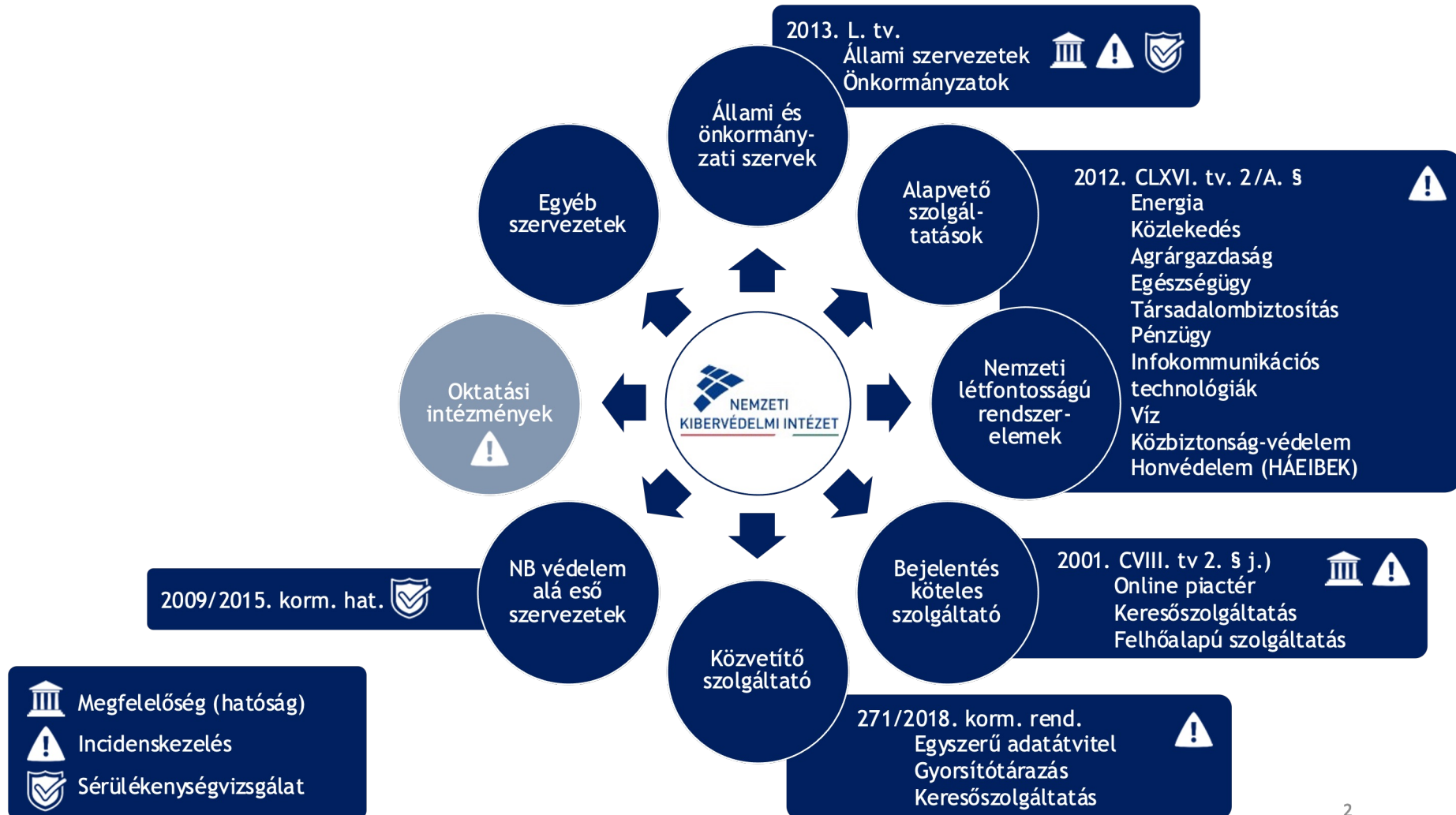
Incidenskezelés



Sérülékenységvizsgálat

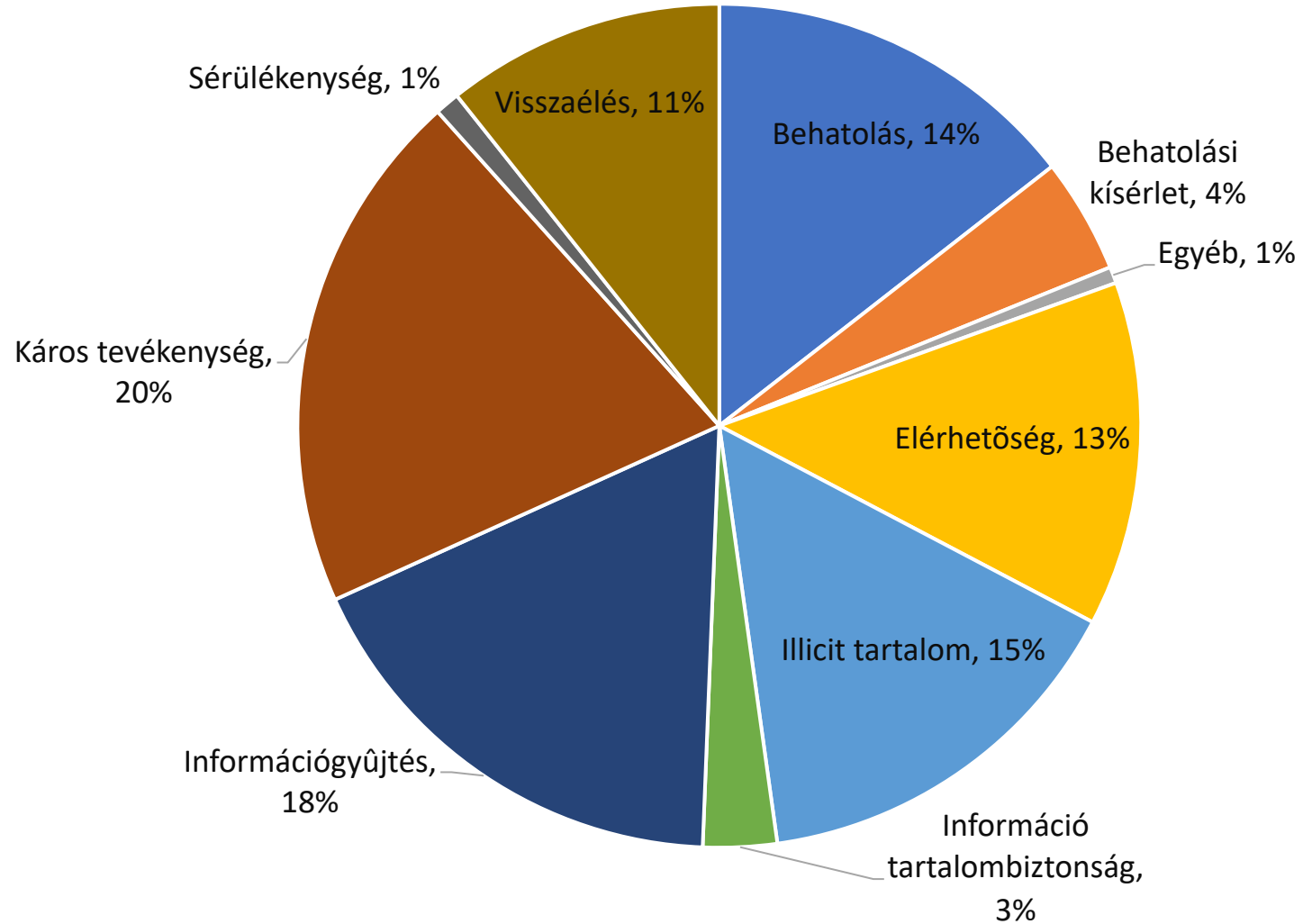


NKI ügyfélköre





Statisztika





Támadók motivációi



- **Script kiddie**
 - Cél: Hírnév, feltűnés, pénz
- **Hacktivismus**
 - Ideológiai motiváció
 - Ideológia közvetítése
- **Kiberbűnözés**
 - Cél: közvetlen anyagi haszonszerzés
 - Pénzügyi és személyes adatok megszerzése
- **Kiberkémkedés**
 - Más országok politikai, gazdasági befolyásolása
 - Szofisztikált támadások
 - Cél: információ

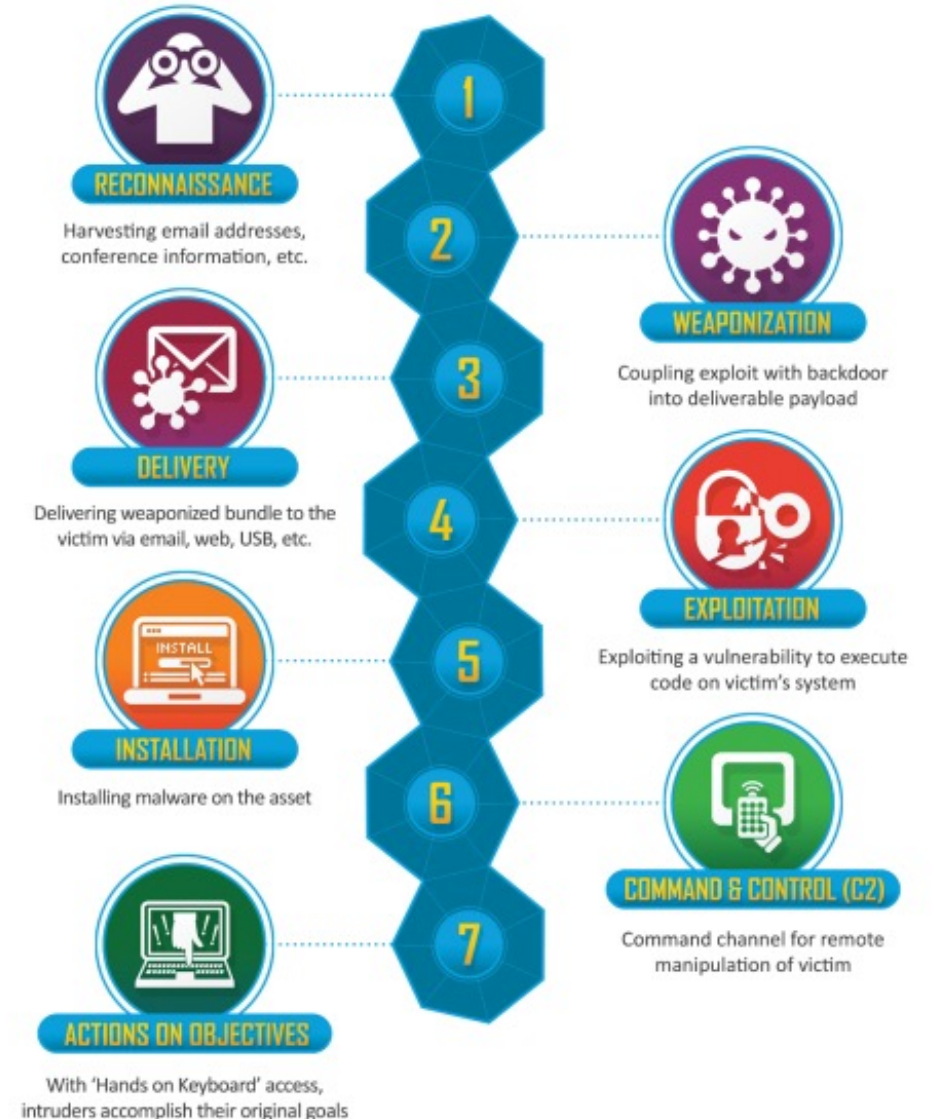




Cyber killchain

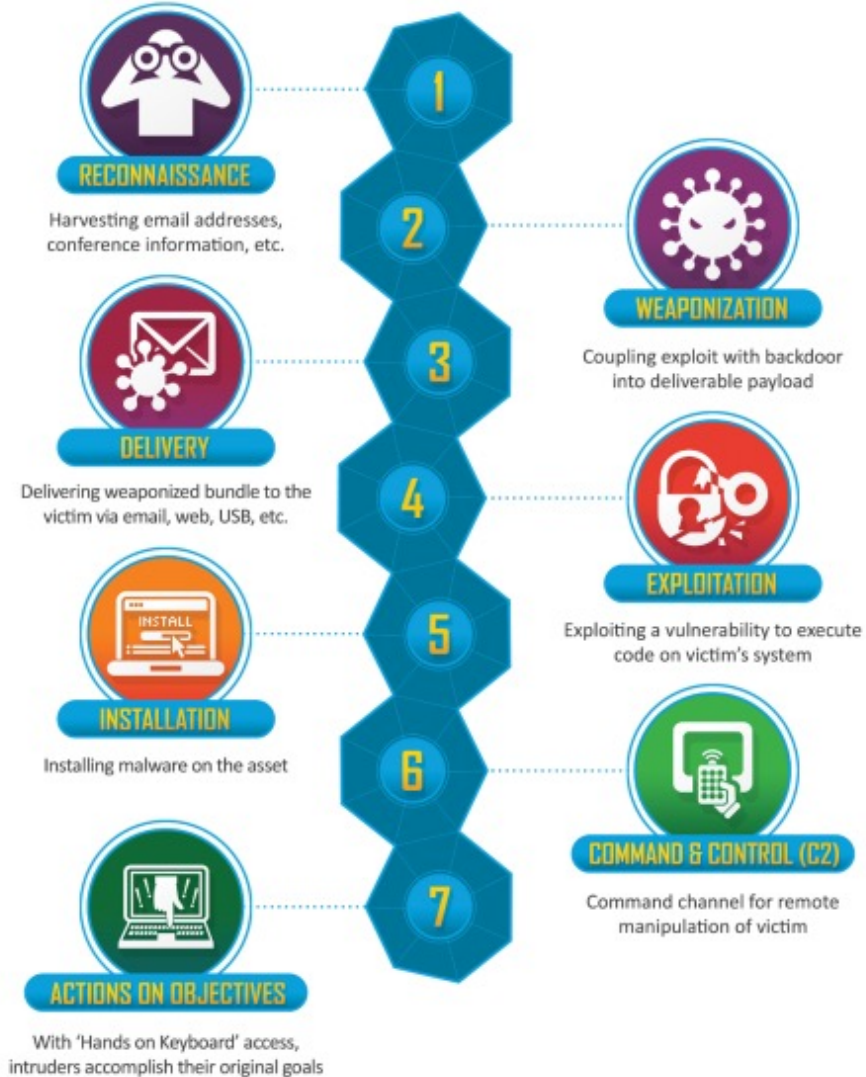
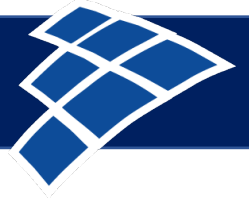


1. Előkészítés
Kutatás
Azonosítás
Támadók kiválogatása
Profilozés
2. Felfegyverzés
Tervezés, eszköz létrehozás
Malware hozzáillesztése a célba juttató eszközhöz (Word, PDF)





Cyber killchain



3. Célba juttatás

Pendrive, e-mail

Ami ellen kevésbé védekeznek

4. Exploitálás

Kód triggerelése

Sérülékenységek kihasználása

5. Installálás

Backdoor telepítése

Perzisztencia kiépítése

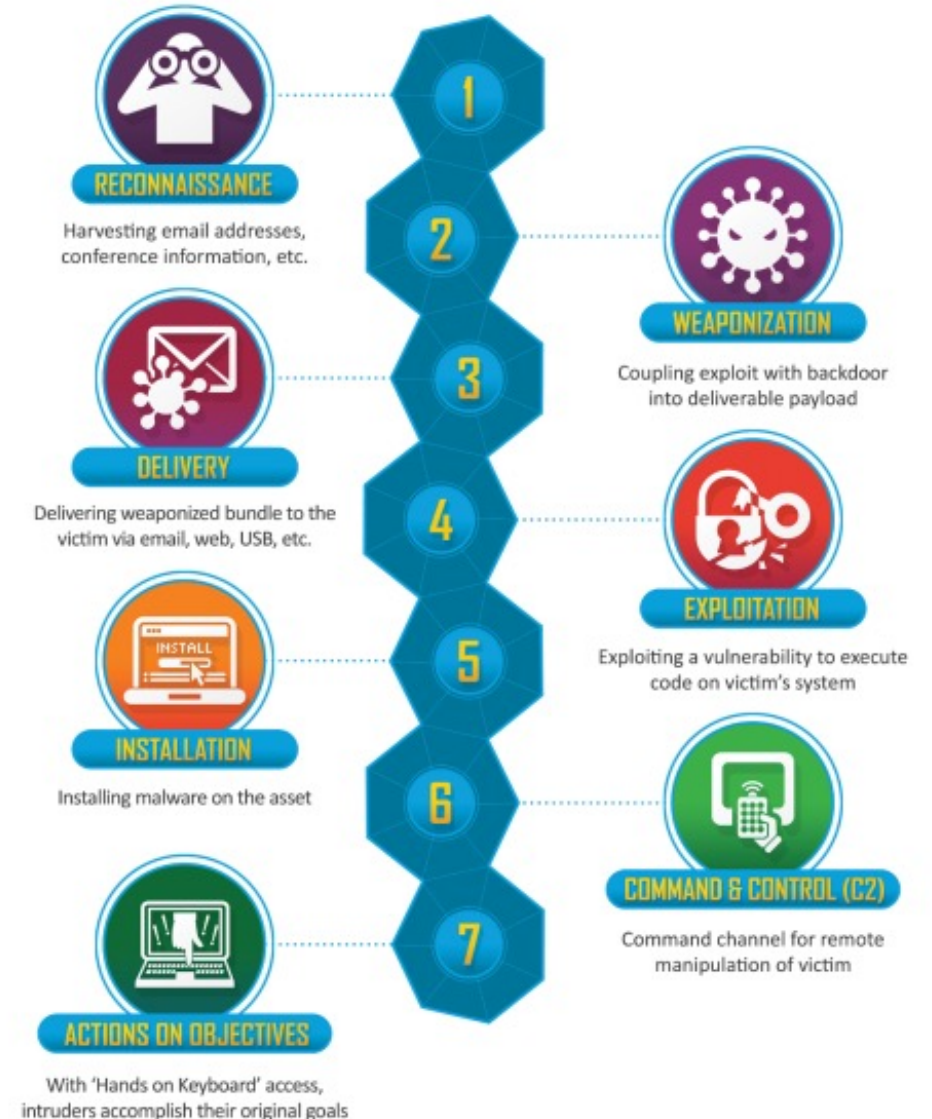
Álcázás



Cyber killchain



- 6. C&C kommunikáció
 - Külső elérés biztosítása
 - Láthatatlanság biztosítása
- 7. Konkrét lépések
 - Adatok elérése
 - Célok elérése
 - Keylogging, szivárogtatás
 - Másik célpont keresése, találása
 - Hosszú ideig jelenlét biztosítása





Adathalászat



- **Célja**
 - Azonosítók (felhasználónevek, jelszavak) megszerzése
- **Módja**
 - E-mail
 - Internetes űrlap
 - (Telefon)
- **Levelek természetete**
 - Minőségük eltérő
 - A cél általában adathalászat
 - Általában nem célzott támadás
 - Forrás beazonosítása nehézkes

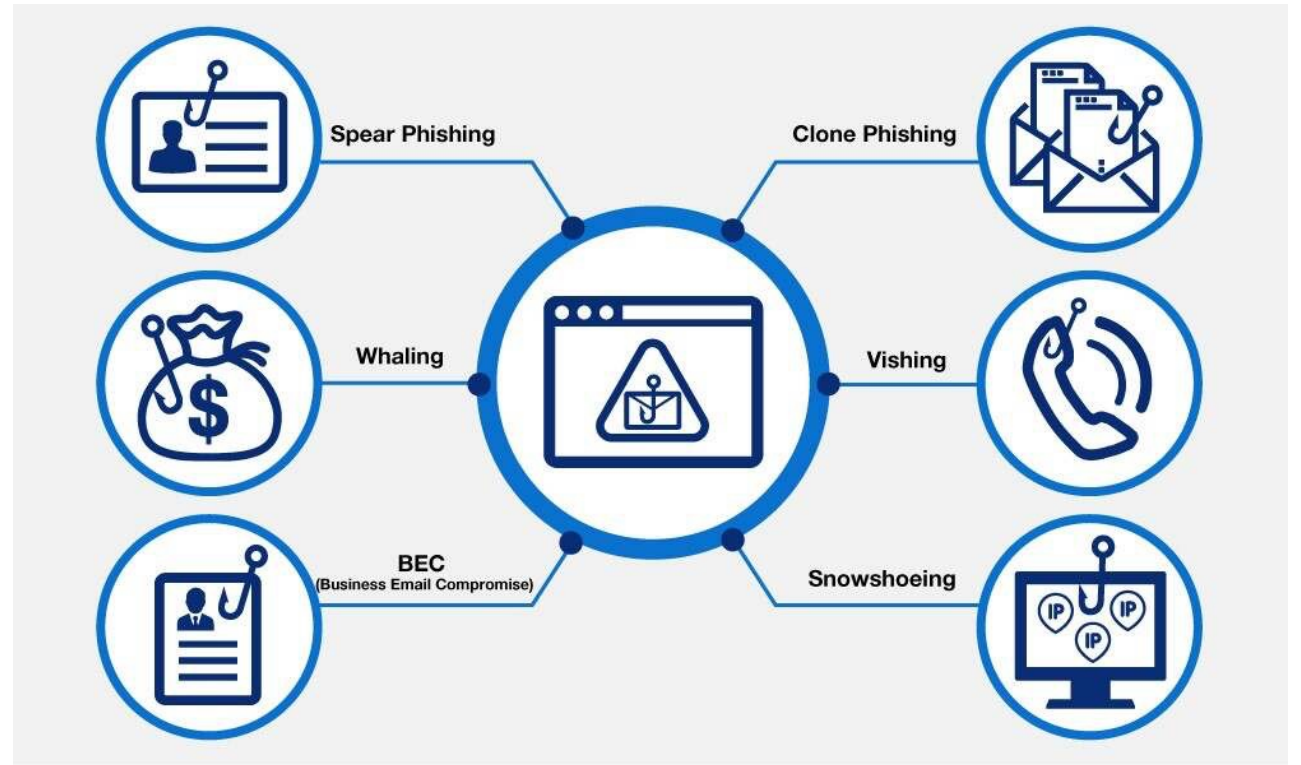




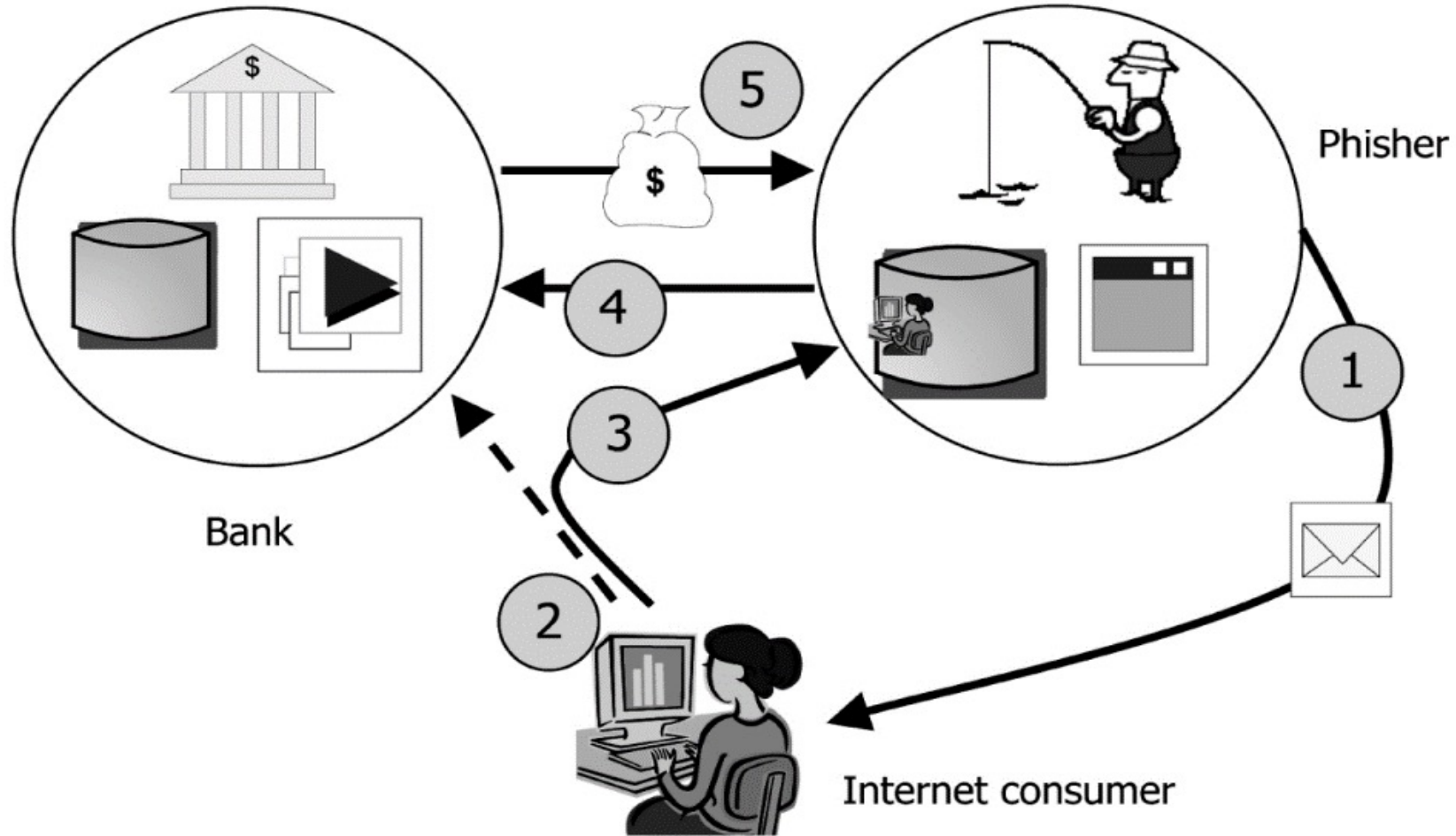
Adathalászat típusok



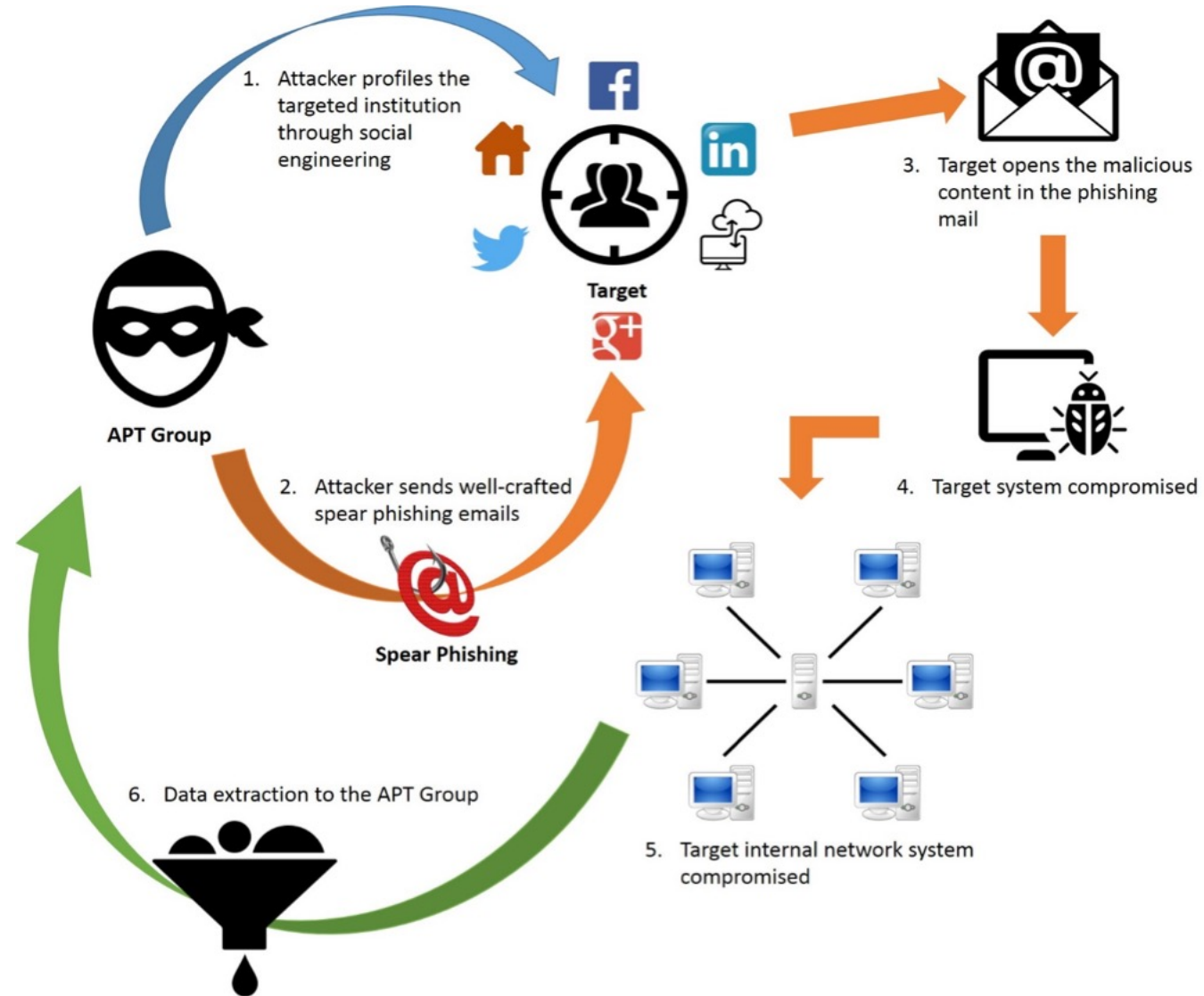
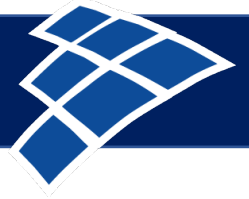
- Célzott adathalászat
- Bálnavadászat
 - CEO
- Business Email Compromise
 - Alternatív bankszámlára kér pénzt
- Klónozás
- Hangos csalás (Voice phishing)
- Hópihe
 - Spam filterek kijátszása kevés email küldésével



Adathalászat séma



Célzott adathalászat séma





Nigériai csalás



Cs 2018.10.18. 0:43

Jean-Pierre Owaoma <jpierreo0021@gmail.com>

Üdvözet,

Címzett

 Eltávolítottuk a fölösleges sortöréseket az üzenetből.

Üdvözet,

Kérlek, nagyon sajnálom, hogy zavarlak. Én azonban Jean-Pierre Owaoma vagyok, én vagyok a személyes ügyvéd egy késő Mr. P.A-nak, az Ön országának állampolgárának, aki itt halt meg az én országomban, a Togói Köztársaságban, és itt egy óriási pénzt hagyott itt egy banknál.

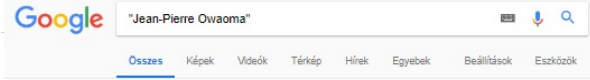
Az összeg 5,7 millió euró. Ha érdekel, hogy segítsék nekem igényelni ezt a pénzt, és küldje el az országomból, kérem, térjen vissza a lehető leghamarabb.

Kösz.

Jean-Pierre Owaoma.



Nigériai család



Nagyjából 124 találat (0,22 másodperc)

Jean-Pierre Owaoma - Lawyer - Jean-Pierre Associates | LinkedIn
<https://www.linkedin.com/pub/jean-pierre-owaoma/48b24596> - Oldal lefordítása
View Jean-Pierre Owaoma's profile on LinkedIn, the world's largest professional community. Jean-Pierre has 2 jobs listed on their profile. See the complete ...

Jean-Pierre Owaoma - Lawyer - J.P Associates | LinkedIn
<https://www.linkedin.com/in/jean-pierre-owaoma-48b24596> - Oldal lefordítása
View Jean-Pierre Owaoma's profile on LinkedIn, the world's largest professional community. Jean-Pierre has 2 jobs listed on their profile. See the complete ...

Jean-Pierre Owaoma | Facebook
<https://www.facebook.com/jeanpierre.owaoma.1> - Oldal lefordítása
Jean-Pierre Owaoma is on Facebook. Join Facebook to connect with Jean-Pierre Owaoma and others you may know. Facebook gives people the power to ...

Jean-Pierre Owaoma - Male » - Friendozle
www.friendozle.com/profile-93181 - Oldal lefordítása
Jean-Pierre Owaoma from is on Friendozle. Friendozle a new place to search for friends, artists, funny video clips, find classmates, socialnetworking, sharing ...

Képtalálatok - "Jean-Pierre Owaoma"



→ További képek a következő kifejezésre: "Jean-Pierre Owaoma" Sánté képek bejelentése

Jean-Pierre Owaoma's Photos » - Friendozle
www.friendozle.com/profile-93181/photo/when_today/ - Oldal lefordítása
Friendozle rate photos, hot or not, upload pics and share with classmates, friends, family in the photo gallery. Friendozle has a total of 0 photo(s).

Jean-pierre Owaoma (Lomé, Togo) | Viadeo
tg.viadeo.com/en/profile/jean-pierre-owaoma - Oldal lefordítása
Jean-pierre Owaoma (Lomé, Togo), occupe actuellement le poste de Lawyer chez:à Jean-Pierre & Associates. Voir son profil professionnel sur Viadeo.

1,009 people > Lome | Togo - Viadeo.com
tg.viadeo.com/en/search/ry/tg/7621/en/?pageNumber=17 - Oldal lefordítása
Jean-pierre Owaoma. Lawyer. Jean-Pierre & Associates. Lomé | Togo. Current job title:Lawyer/Jean-Pierre & Associates. School: Université De Lomé ...

419 scam: Barrister Jean-Pierre Owaoma <jpierreo20@gmail.com ...
www.419scam.org/emails/2015-05/05/00837220.351.htm - Oldal lefordítása
From: Barrister Jean-Pierre Owaoma <jpierreo20@gmail.com> Reply-To: jpierreo20@outlook.fr. Date: Mon, 4 May 2015 20:59:39 +0000. Subject: Greetings.

Jean-Pierre Owaoma - Google-
<https://plus.google.com/106206155279071183205> - Oldal lefordítása
Jean-Pierre Owaoma - Google+. ... Jean-Pierre Owaoma. About Posts. Looks like you've reached the end. Looks like you've reached the end. Unable to load ...





Nigériai csalás



--

Irodánk elérhetősége: 2554 Road Of Kpalime Face Pharmacy Bet, Lome, Gulf.

Ez a WU bank igazgatója értesíti Önt arról, hogy a Nemzetközi Valutaalap (IMF) 850 000,00 USD kártérítést fizet Önnek, mert megtalálta az Ön e-mail címét a csalás áldozatainak listáján. Hajlandó vagy venni ezt az alapot vagy sem?

Sürgősen várjuk a hírt.

Tisztelettel

Tony Albert

BANKIGAZGATÓ

Lépjén kapcsolatba a Whatsappal, +22892905783



Sextortion



Este mensaje parece peligroso

Los ladrones de información personal usan mensajes parecidos. Evita hacer clic en enlaces, descargar archivos adjuntos o responder con información personal.



I am aware [redacted] is your pass word. Lets get directly to the purpose. You don't know me and you're probably thinking why you are getting this e mail? No-one has paid me to check about you.

actually, I placed a malware on the X vids (sexually graphic) web site and do you know what, you visited this site to have fun (you know what I mean). While you were viewing videos, your internet browser began operating as a Remote Desktop with a keylogger which gave me access to your display and web camera. Immediately after that, my software program gathered your complete contacts from your Messenger, Facebook, as well as emailaccount. Next I made a double video. 1st part displays the video you were watching (you've got a fine taste hehe), and 2nd part shows the recording of your web camera, and its you.

You have just two options. We should explore these types of options in details:

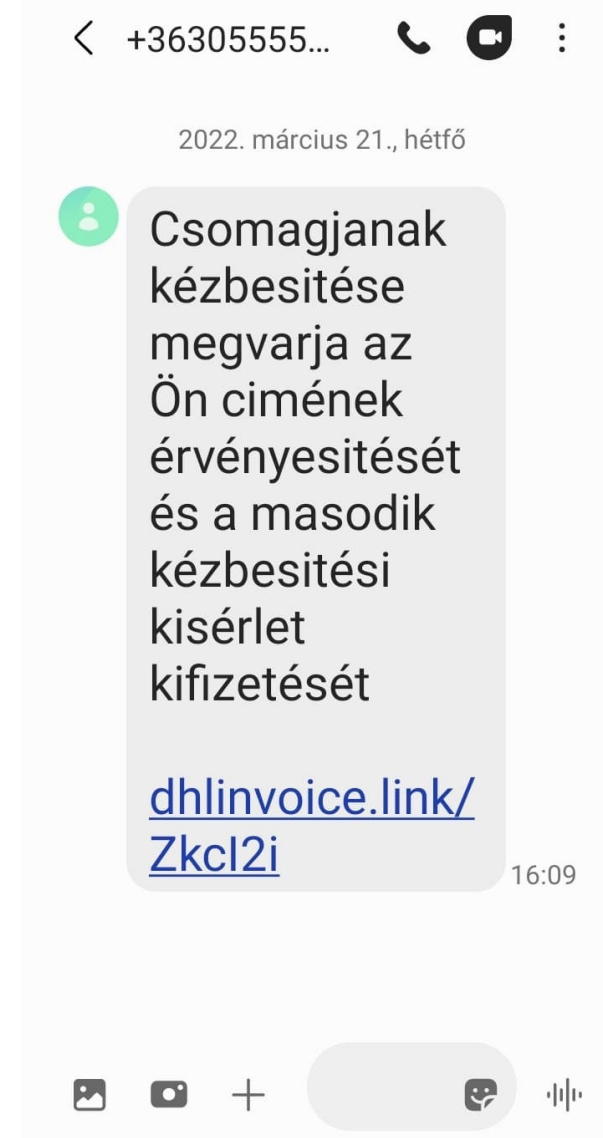
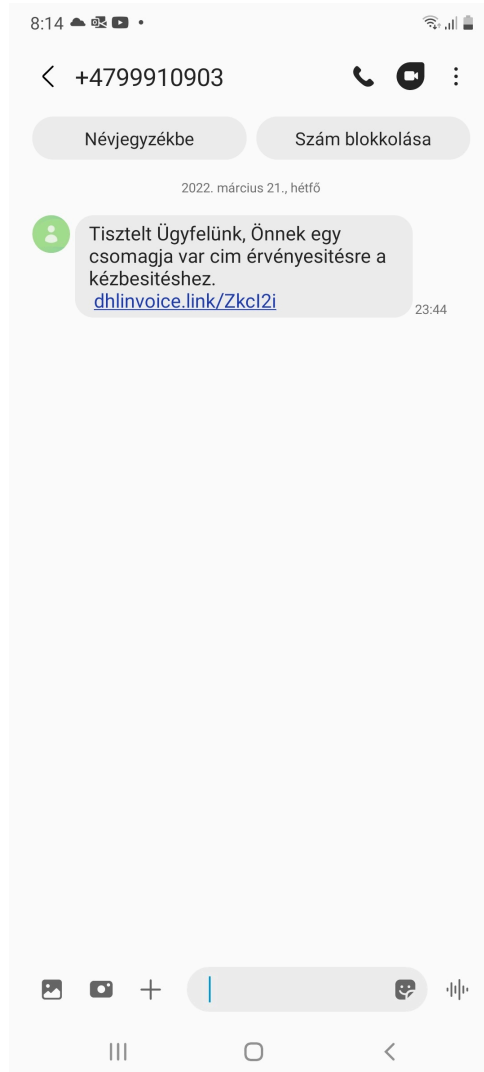
Very first choice is to just ignore this e-mail. As a consequence, I will send out your very own videotape to just about all of your contacts and also consider regarding the humiliation you will definitely get. Moreover in case you are in a committed relationship, just how it can affect?

Next choice should be to pay me \$5000. Let us regard it as a donation. In this case, I most certainly will instantaneously eliminate your videotape. You will continue on with everyday life like this never occurred and you will not ever hear back again from me.

You will make the payment via Bitcoin (if you do not know this, search for "how to buy bitcoin" in Google).



Phishing példák





Phishing példák



Ügyfélkapu

onlineszamlam- nav.com/digi/ugyfelkapu/simplepay/index.php?id=bb3b4e7df0bb3c494e57c9eaf7749caccountry=HU/_DIGI_kft

DIGI

f in YouTube Instagram

KIFIZETENDŐ SZÁMLÁK ÖSSZESÍTÉSE

Egyenlítsse ki számláját azonnal, bankkártyája segítségével.

DIGI + invitel simplepay by OTP Mobil

Mastercard Maestro VISA VISA

Sorszám	Számla kelte	Fizetési határidő	Számla értéke	Fizetendő
4796038	2021-02-03	2021-02-28	6299 Ft	6,299 Ft
Összesen				6,299 Ft

Kérjük adja meg e-mail címét, ahova a visszaigazolást kéri

E-mail cím

Tudomásul veszem, hogy a(z) DIGI Távközlési és Szolgáltató Kft (1134 Budapest, Váci út 35) adatkezelő által a(z) <https://ugyfelkapu.digi.hu> felhasználói adatbázisában tárolt alábbi személyes adataim átadásra kerülnek az OTP Mobil Kft., mint adatfeldolgozó részére. Az adatkezelő által továbbított adatok köre az alábbi: E-mail cím

Elfogadom

BANKKÁRTYÁS FIZETÉS INDÍTÁSA

Tájékoztató

KAPCSOLAT

Süti beállítások

DIGI DIGIonline DIGI sport DIGI NOW DIGI WORLD DIGI Life DIGI ANIMÁL WORLD

f in YouTube Instagram



Phishing példák



SimplePay x +
onlineszamla-nav.com/digi/ugyfelkapu/simplepay/pay/

simplepay by OTP Mobil

BANKKÁRTYÁS FIZETÉS

Nyelv: MAGYAR

VISSZA A KERESKEDŐ OLDALÁRA

DIGI DIGI Távközlési és Szolgáltató Kft.

ÖSSZESEN: 6 299 HUF

VISA

Kártyaszám

Kártyabirtokos neve

HH/ÉÉ CVC/CVV kód

FIZETÉS

Ügyfélszolgálat
Telefonszám: +36(1)366-6611 | +36(20)366-6611 | +36(30)366-6611 | +36(70)366-6611
Email: ugyfelszolgalat@simple.hu

Fejlesztő és üzemeltető az **otp Mobil**



Phishing példák



From: DPD

Sent: Sunday, January 17, 2021 3:35 PM

To: budaventura@budaventura.hu

[lookup email](#)

[lookup "budaventura.hu"](#)

Subject: [ob6xp6dy1qvry98j]

Szia, budaventura@budaventura.hu

[lookup email](#)

[lookup "budaventura.hu"](#)

További részletekre van szükségünk a csomag újbóli kézbesítéséhez, mint a megadott cím hiányosnak tűnik.

Kérjük, adja meg a teljes információt ehhez a címhez, hogy megkísérelje az újratöltést.

Csomagját jelenleg a helyi raktárunkban tároljuk.

Ha azonban a művelet nem történik meg 48 órán belül, akkor azt visszaküldik az eredeti feladónak.

>>>> Frissítse a visszaszállítási címet <<<<<

DPD @ 2021




Phishing példák




Browser address bar: <https://www.posta.hu.mitmom.com/flower774659/>

Navigation: Magánszemélyek | Üzleti partnerek | **ÉNPOSTÁM** | Belépés | Kosár (0) | HU

Magyar Posta | KÜLDEMÉNY FELADÁSA | KÜLDEMÉNY ÉRKEZÉSE | BE- ÉS KIFIZETÉS | PÉNZÜGYI SZOLGÁLTATÁSOK | KÖZMŰ ÜGYINTÉZÉS | BÉLYEG | ÚJSÁG | EGYÉB | **WEBSHOP**


 **Azonosító szám: 97357445**
(Expressz csomag)

 **Fizetési részletek :**

Címsor * város * postai

Teljes név *

telefonszám*

 **További szállítás**
805,28 HUF
(Tartalmazza az ÁFÁT)

Teljes : **805,28 HUF**
(Tartalmazza az ÁFÁT.)

-----Eredeti üzenet-----
Dátum: 2022. február 23., szerda, 09:35:27
Feladó: "Magyar Posta."
Tárgy: A Magyar Posta tájékoztatta, hogy az Ön szállítása: 97357445HU
Címzett: undisclosed-recipients@ismeretlen

Tisztelt Ügyfelünk,

A Magyar Posta tájékoztatta, hogy az Ön szállítása: 97357445HU, és díjfizetésre vár
Díjak: 805,28 HUF
Dátum : 02/24/2022.
Küldd el a csomagomat

2022 © - Posta all rights reserved



Phishing példák



Browser address bar: https://magyar-post.web.app/Confirm_Delivery?Customs-Clearance=1U93HI81YI8YDZ

Magyar Posta Kosár (1)

Csomagjaim - 1 csomag

	Csomag továbbítás PACK#2572077179 Súly: 1,7 kg Mennyiség: 1	795 Ft
--	--	---------------

Várható kézbesítési dátum
27/03/2022 - 29/03/2022

Válasszon fizetési módot

VISA AMERICAN EXPRESS Mastercard PayPal

Összegzés

Töltse ki adatait

Ország: Magyarország



Phishing példák



MKB BANK Net**BANK**ár

SECURED BY SECTIGO

MKB BANK Nyrt.
Székhely: 1056 Budapest, Váci u.38.
Cégjegyzék helye és száma:
Pótvárosi Törvényszék Cégbírósága,
Cg. 01-10-040952

MKB TeleBANKár:
Lakossági ügyfélszolgálat: 06 (80) 333-660
Vállalati ügyfélszolgálat: 06 (80) 333-770
Külföldi: +36-1-373-3333

Bejelentkezés

Azonosító:

Jelszó:

[Elfelejtette a jelszavát?](#) [Bejelentkezés](#)

Új NetBANKár szerződés igénylése

Biztonság | Kondíciók | Támogatott böngészők | Hírvé | Kapcsolat
Adatvédelmi irányelvek | Általános üzleti feltételek | Jogi nyilatkozat | Impresszum

Swift: MKKB HU HB
MKB BANK Nyrt., 1056 Budapest, Váci u.38.

Tisztelt Ügyfelünk,

Kaptál egy új üzenetet MKB Bank.

Üzenet megtekintése.

Köszönjük, hogy velünk Banking.

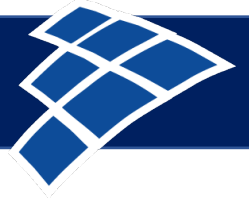
--

Üdvözlettel,
MKB Bank Zrt

© 2021 MKB Bank Zrt.



Phishing példák



Információ a kifizetett adók egy részének visszaszerzéséről.

Adók visszatérítése.
Miután áttekintette a 2018-tól fizetett összes adót, megkérjük a nevét, családi nevét és azonosító számát. A hivatal ügyfélszolgálatán keresztül, illetve postán, adószámla-kivonaton értesíti az adózókat, ha túlfizetésük van.

Információ szükséges.

Teljes név :

Azonosító szám :

E-mail :

Lekérdezés

A NAV weboldalai szerzői jogvédelem alatt állnak.
A honlapon szereplő információk változatlan tartalommal és formában szabadon terjeszthetők.

[Kapcsolatfelvétel](#) | [Archív oldalak](#) | [További honlapok](#) | [Adatvédelmi tájékoztató](#) | [Impresszum](#) | [Közadatkereső](#)
1054 Budapest, Széchenyi u. 2.

Tisztelt Ügyfelünk!

Az idén kifizetett összes adót az online ügyfelek számára ellenőrizték. Az év végén jelentkezzen be az alábbi linkre, és hajtsa végre az alábbi lépéseket: Adja meg nevét, vezetéknévét és azonosítószámát, és erősítse meg e-mailjeit. Biztosítjuk, hogy jogod van az ebben az évben fizetett pénz visszaszerzésére

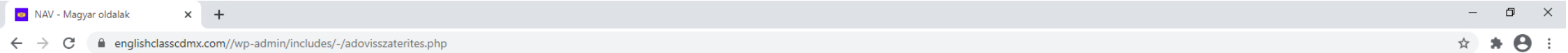
Ellenőrizze most


Kérem jelentkezzen be az adóvisszatérítési oldalra, hogy visszaigényelheti az alapokat.

Kiemelt figyelemre számíthatnak a virágot, koszorút és mécseseket árusítók. A NAV munkatársai a nyugta- és számlaadást, az online pénztárgép megfelelő üzemeltetését, valamint az alkalmazottak bejelentését vizsgálják.




Phishing példák





Nemzeti Adó-
és Vámhivatal




Visszatérítési információ.

Név: dzaadazd
Azonosítószám: 67576587587
Részletek:
Visszatérítési összeg: 73215 Ft
dátum: 02/2018

A visszaváltás befejezése után a hitelkártyán lévő összeg 10-15 napon belül jóváírásra kerül.

A hitelkártya adatait.

Kártyaszám : 

Lejárat dátum (hh/é) :

Érvényesítési kód (CVC2/CVV2)

ez az információ csak a NAV-ra térít vissza. Ezt a részletet megtérítjük, kérjük, győződjön meg róla, hogy minden helyes

[Tovább](#)

A NAV weboldalai szerzői jogvédelem alatt állnak.
A honlapon szereplő információk változatlan tartalommal és formában szabadon terjeszthetők.

[Kapcsolatfelvétel](#) | [Archív oldalak](#) | [További honlapok](#) | [Adatvédelmi tájékoztató](#) | [Impresszum](#) | [Közadatkereső](#)
1054 Budapest, Széchenyi u. 2.



Phishing példák



NKM Energia - Földgáz Online Ü... x

energiazrt.nkm.com/pages/aram/index.php?id=f61a8ec7f4b74f7130e8f861d089c8c2country=HU/_Nkm_Zrt

NKM Energia Zrt. | Nemzeti Közművek | Elérhetőségek | ⚠ Gázzzivárgás-bejelentés

NKM ONLINE ÜGYFÉLSZOLGÁLAT

Regisztráció
Elfelejtett jelszó
Időpontfoglalás
Fizetési feltételek
Mérőállás díktálása

BANKKÁRTYÁS SZÁMLABEFIZETÉS

TELJES NÉV :

Kártyaszám :

CVC/CVV kód :

Lejárat dátum (MM/YY) :

TOVÁBB

megerősít Kérjük add meg a fizetéshez használni kívánt kártya adatait

Tisztelt Ügyfelünk!

Elkészült az új földgázszámlája.

A számla főbb adatai:

Számla bruttó értéke: 5.852 HUF
Számla végösszege: 5.852 HUF
Fizetési határidő: 2020.12.28.

Szerződéses folyószámla száma: 10203958
Felhasználó azonosító száma: 5014003570
A számla fizetendő összegét a bankkártyás fizetés linkre kattintva tekintheti meg.

Utaláshoz szükséges adatok:
Bankszámlaszám: 10300002-20580731-49020647
Számla sorszáma (közleménybe): **100725941389**

Azonnali, bankkártyás kifizetéséhez kattintson a következő linkre: [Bankkártyás fizetés](#)

Üdvözlettel
NKM Online ügyfélszolgálat - földgáz

Ez egy rendszer által küldött üzenet kérjük, ne válaszoljon rá!
Tájékoztatjuk, hogy az erre a címre küldött értesítéseket nem tudjuk feldolgozni.

Ügyfélszolgálati elérhetőségek

Ez az elektronikus levél (e-mail) és a hozzá kapcsolt mellékletek, fájlok (a továbbiakban együtt: Üzenet) kizárólag a Címzett(ek)nek szólnak. Az Üzenetben foglalt információk bizalmasak lehetnek, melyeknek titokban maradásához az NKM Energia Zrt.-nek (a továbbiakban: Társaság) jogilag és üzletileg méltányolható érdeke fűződik. Amennyiben valamely hiba folytán vagy tévedésből Ön nem az Üzenet címzettje, továbbítania, közölnie vagy bármely részét felhasználnia. Ebben az esetben szíveskedjen az Üzenetet és minden másolatát törölni és haladéktalanul értesíteni a küldőt.

Jogi nyilatkozat | Impresszum | Segítség a használathoz | Adatvédelmi információk

CIB BANK



Phishing példák



Tisztelt Ügyfelünk!

Elkészült az új földgázzámlája.

A számla főbb adatai:

Számla bruttó értéke: 1.340 HUF

Számla végösszege: 1.340 HUF

Fizetési határidő: 2021.01.15

A számla fizetendő összegét a bankkártyás fizetés linkre kattintva tekintheti meg.

A számla részletes adatait a NKM Online Ügyfélszolgálat Számlázás - Számlák lekérdezése menüpontban tekintheti meg.

Azonnali, bankkártyás kifizetéséhez kattintson a következő linkre:

Bankkártyás fizetés

Esetleges kérdésével forduljon bizalommal ügyfélszolgálatunkhoz!

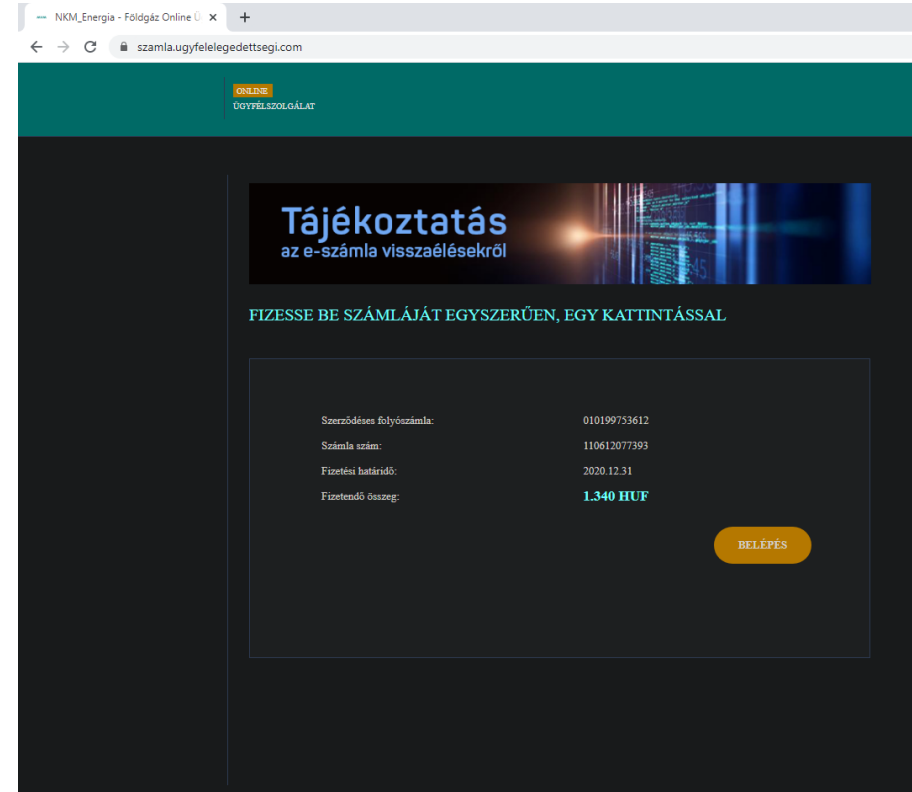
Üdvözlettel

NKM Online ügyfélszolgálat - földgáz

Ez egy rendszer által küldött üzenet kérjük, ne válaszoljon rá!


Tájékoztatjuk, hogy az erre a címre küldött értesítéseket nem tudjuk feldolgozni.

Ügyfélszolgálati elérhetőségek






Phishing példák



Security Challenge

Please type the characters you see in the image for security purposes.



[I'm not a robot](#)

HU

PayPal

Jó nap,

Tranzakciós kérelmet kaptunk pénz befizetésére az alább felsorolt online pénztárcákban

Skrill és Neteller a kártyád használatával, amely összekapcsolódott a PayPal-számláddal. Ezért volt

tegye vissza a tranzakciós kérelmet, és 48 órán keresztül adjon hozzá korlátozást PayPal-számlájához.

Ha Ön volt a tranzakció tulajdonosa, kérjük, ne csináljon semmit, és hagyja figyelmen kívül ezt az üzenetet.

A PayPal mindkét pénztárca visszaigazolja a tranzakciós utalást (Skrill és Neteller)

ha nem, kérjük, kövesse ezeket a következő lépéseket az ügylet visszavonásához és az azonnali visszatérítés kéréséhez

Fontos figyelmeztetés: automatikus rövid üzenetet küld a telefonszámra, amely tartalmazza egy kód a jogosulatlan tranzakció törlési folyamatának befejezéséhez.

A visszatérítés iránti kérelem teljesítéséhez be kell írnia az SMS-kódot, a kódot

tartalmazza a felhasználít összeget.

Az alábbi linke kattintva törölnie kell a tranzakciót és kérnie kell a visszatérítést.

Vissza a pénzemet

Figyelem: Ez az e-mail automatikusan jön létre, és nem az ügyfél és a PayPal közötti kommunikációra szolgál.

Köszönöm a megértést



Phishing példák



Lakossági üzleti Bolunk

KESZULEKEK SZOLGALTATASOK UGYINTEZES

BELEPES

BELEPES ONLINE UGYINTEZESHEZ

A belepeshoz e-mail-cim, mobiltelefonszam, MT ügyfel-azonosito vagy üzleti felhasználonev, valamint a hozzajuk tartozo jelszo szukseges.

Belepési azonosító [Milyen azonosítót használnak?](#)

Jelszo [Nem tudom a jelszavam](#)

Belepve maradok

Belepek

Nincs meg Telekom fiokod?

Hozz létre Telekom fiokot, lépj be egyszerűbben, és kezeld együtt előfizetéseidet!

Telekom fiokot regisztrálok

EGYÜTT.VÉLED

© 2017 Magyar Telekom Nyrt. [Jogi tudnivalók](#) [Általános szerződési feltételek](#) [Adatvédelem](#) [Fejl](#)

TISZTELT ÜGYFELÜNK

A számlát nem fizették még :

Folyószámla : 363451069.

Számla sorszám : 5130182015337201

Fizetési határidő : 12/01/2021

Státusz : Befizetésre vár

Számlázott összeg : 1.315 Ft

Remeljük, hogy a számla kifizetése a megadott határidőn belül. Vagy az eA-fizetés velünk automatikusan kikapcsol

Most már fizetni a számlát egyszerű és sima utat a bankkártya vagy a bankszámla és biztonságosan

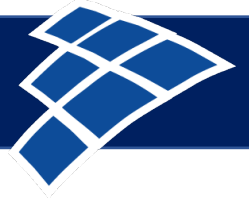
Kérjük, kövesse az alábbi linket a folyamat befejezéséhez

<https://www.telekom.hu/telekomfiok/belepes?6...../Token=252MSBTKL55....ID> [lookup "www.telekom.hu"](#)

©2021 Magyar Telekom Nyrt.



Phishing példák



10:24 Üzenetek 4G

maftill.com

Gratulálok!!!

Ma te vagy a kiválasztott győztes!!!

☆ Tesco Ma 10:21

TESCO

Üdvözlöm Miklós. Az iPhone 12 a Kézbiztosítási pontnál van. A 2021-es Tesco Tesztelési Program részeként ön lett a tökéletes jelölt a legújabb iPhone 12 tesztelésére és megtartására. Kattintson erre a linkre, hogy az iPhone 12 www.tesco.hu/2021program

Üdvözlettel,
Szolgáltatások Tesco

13:46 4G

+47 999 10 903 >

máj. 30., Szo 13:29

G-882220 – az Ön Google ellenőrző kódja.

nov. 24., K 13:16

Miklos thank you for your patience! We dep0sit 300 EUR to your acc0unt. please register here: <https://mnglj.com/5tq> and collect your earnings.

nov. 25., Sze 10:15

Kedves vasarlo! Ez a 3-ik emlekezteto a 11.24-i sorsolason nyert termekrol. Szerezze meg itt: xd7.link/RPzM7

ma 10:21

Kedves vasarlo, van (1) Tesco csomagod varakozasban. Kerjuk ellenorizd es igazold vissza: lr5.link/WTj6G

Szöveges üzenet



Phishing példák



Kedves Ügyfelünk!

Aktuális havi (korábbi UPC vezetékes vagy mobilszolgáltatás) elektronikus számlád elkészült, melynek részleteit az alábbiakban küldjük számodra.

Amennyiben számládat már rendezted, kérjük, üzenetünket tekintsd tárgyatlannak. A csekkes befizetés 3-4 munkanap, az utalás 1-2 munkanap amíg könyvelődik.

Számla alapján fizetendő: 14889Ft

Fizetési határidő: 2020-12-29

Számla kelte: 2020-12-11

Számla sorszáma: 834813026

Ügyfélszám: 0029126380

Iktatószám: CC-5865118/2-2020

A számla összege az aktuális havi tételek összegét tartalmazza, az esetleges korábbi túlfizetéseidet vagy számlaelmaradásaidat nem.

Kérjük, ne feledd, hogy amennyiben e-Pack tarifával rendelkezel, a kedvezmény igénybevételének feltétele, hogy a fizetendő összeget internetes bankkártyás fizetéssel, átutalással, OTP bankautomatán keresztül vagy csoportos beszédési megbízással egyenlítsd ki. Banki átutalás esetén a(z) 104100220029126380000102 számlaszámot használd, a közlemény mezőben tüntesd fel az ügyfélszámodat: 0029126380.

Elérhetőségeink

E-mail: www.vodafone.hu [lookup host](#) /kapcsolat

Telefonszám: 1270

Külföldről hívható telefonszám: +36 1 288 1270

Levelezési cím: 1476 Budapest Pf.303

Üdvözzettel:

Vodafone

Ezt a levelet a Vodafone Magyarország Zrt. küldte tájékoztató jelleggel. A Szolgáltató az adataidat bizalmasan kezeli. A levél tartalmáért a Szolgáltató felelős.

Személyes adataid kezeléséről további információért keresd fel a Vodafone Adatvédelmi



Zsarlóvírusok



- Zsarlóvírus: A zsarolóvírus egy olyan típusú **támadás**, amelyben a támadók átveszik az **irányítást** a célpont eszközei felett, és **váltságdíjat** követelnek cserébe az **eszköz elérhetőségének visszaállításáért** és **titkosságáért**.





Zsarlóvírusok típusai



A zsarolóprogramok négy alapvető műveletet hajthatnak végre:

- zárolás
- titkosítás
- törlés
- lopás

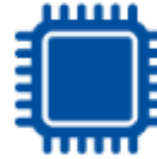




Zsarolóprogram által megcélzott előforrások



- Fájlok
- Mappák
- Memória
- Adatbázis
- Kijelző
- MFT
- MBR
- Felhő
- CMS





Zsarolóvírus életciklusai



- Kezdeti hozzáférés
 - hozzáférés megszerzése
 - biztonsági szoftver letiltása
 - helyreállítási funkciók leállítása
 - zsaroló program telepítése





Zsarolóvírus életciklusai



- **Végrehajtás**
 - célpont tanulmányozása
 - további gépekre terjedés





Zsarolóvírus élelciklusai



- **Cél** megvalósítása
 - Eszköz elérhetőségének vagy titkosságának megtámadása





Zsarolóvírus életciklusai



- Zsarolás (ransom)
 - Kommunikáció
 - Fenyegetés
 - Követelés

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View 95 20 15 Next >>

RANSOMWARE ATTACK

You only have 3 days to submit the payment, or your files will be lost

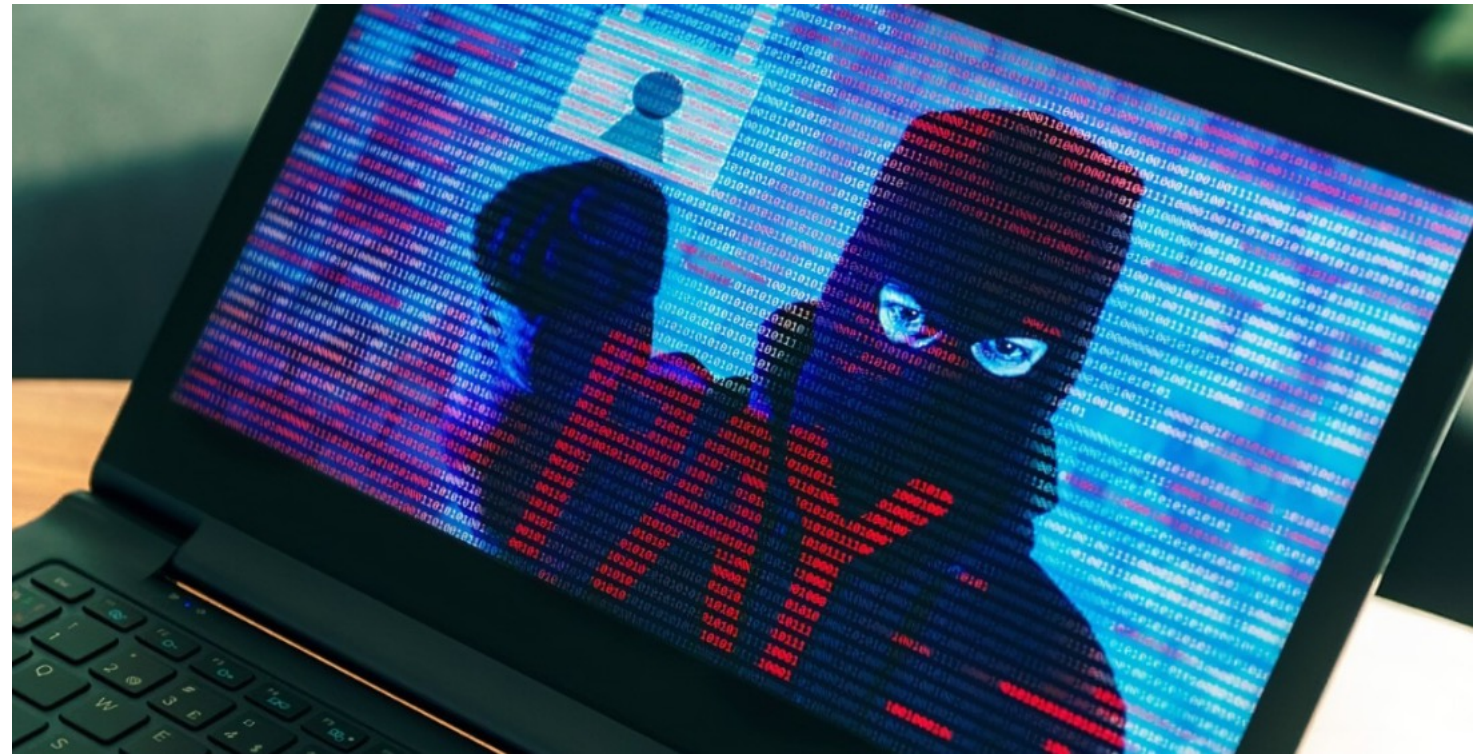
Time Left
02:23:59:06



Váltságdíj tárgyalások



- Privát kommunikáció a célpont és a támadó között (nem ajánlott lépés)
- Két kimenetel:
 - Célpont kifizeti a váltságdíjat
 - Nem fizeti ki a célpont a váltságdíjat

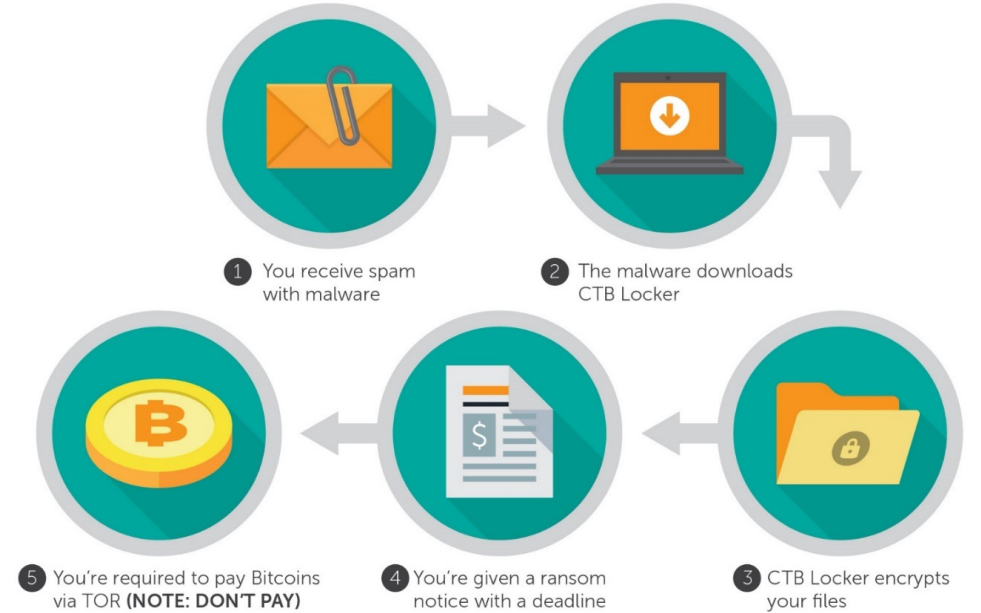




Zsarolóvírus terjedése



- „Szokásos módon”
 - E-mailben
 - Csatolmány vagy URL segítségével
 - Sérülékenység kihasználásával
- Új támadási formák
 - RDP-n keresztül
 - TeamViewer segítségével
 - Nem titkosítanak - jelszavas archívek használata
 - Az alkalmazás rendelkezésre áll a szerveren
 - A károkozás így is megtörténik



RDP = Ransomware Deployment Protocol



A leghíresebb



- Wanacry 2017
- Kb 230 000 áldozat 4 nap alatt
- Lazarus csoport - KNDK
- Windows SMB sérülékenység
- Eternal blue – NSA
- Áldozatok (milliárd dollár)
 - Nissan
 - Renault
 - Tekefónica
 - FedEx
 - Deutsche Bahn
- Kill switch (titkosítás és terjedés)

Wana Decrypt0r 2.0

Ooops, your files have been encrypted! English

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on 5/16/2017 00:47:55
Time Left 02: 23: 57: 37

Your files will be lost on 5/20/2017 00:47:55
Time Left 06: 23: 57: 37

About bitcoin
How to buy bitcoins?
Contact Us

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

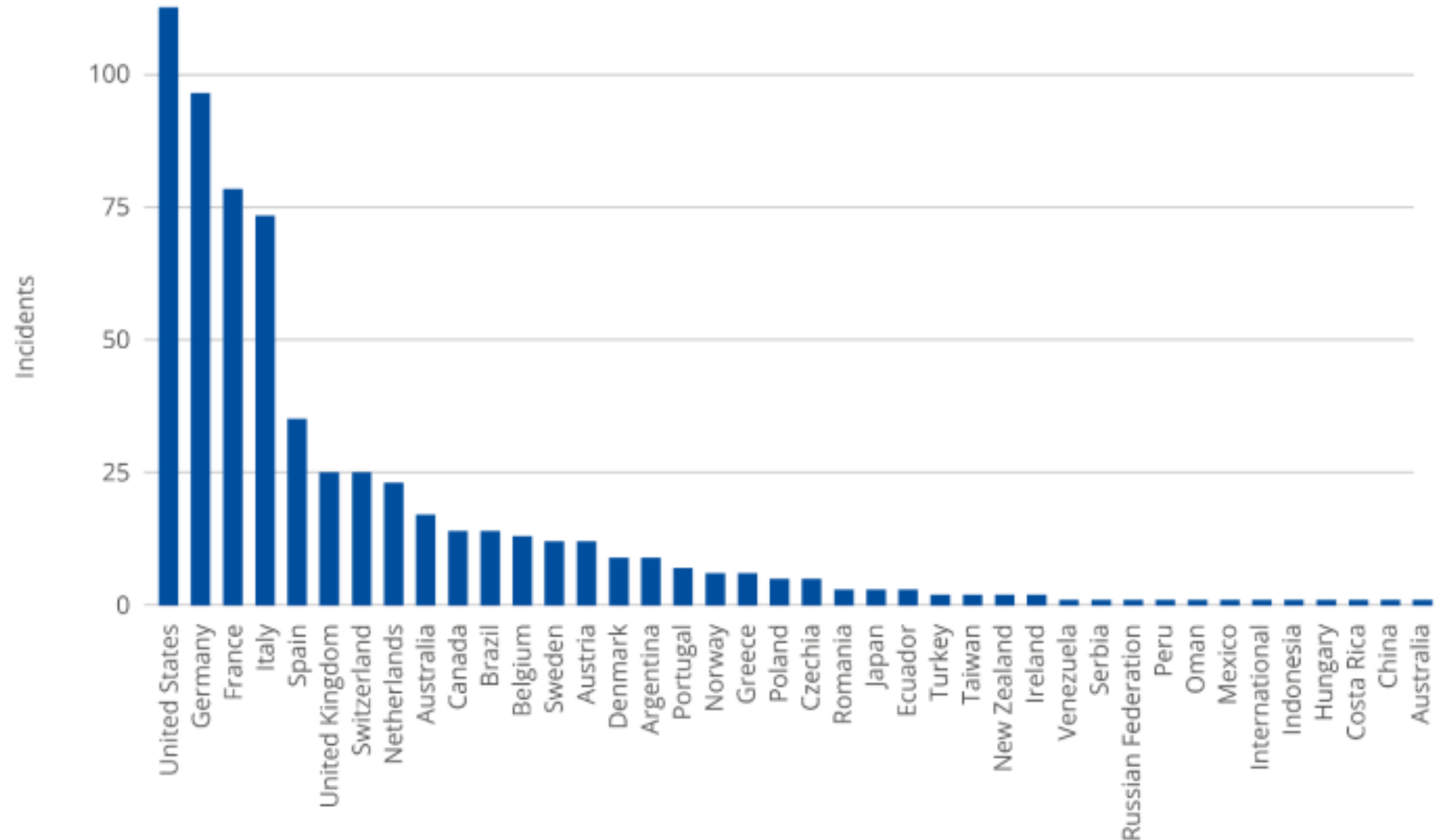
Check Payment Decrypt



Zsarolóvírus incidensek analízise



- A zsarolóvírus incidensek száma országonként 623 elemzett incidens alapján

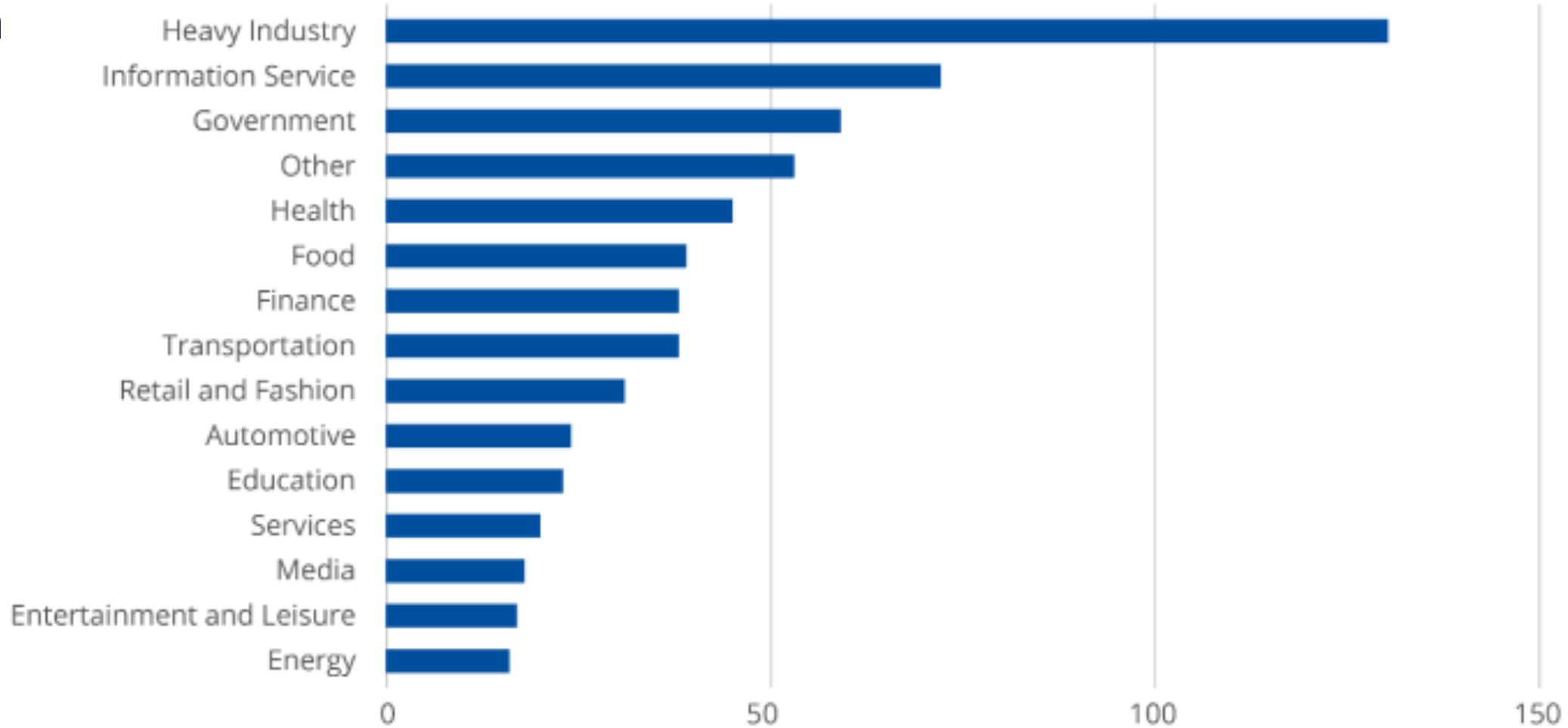




Zsarolóvírus incidensek analízise

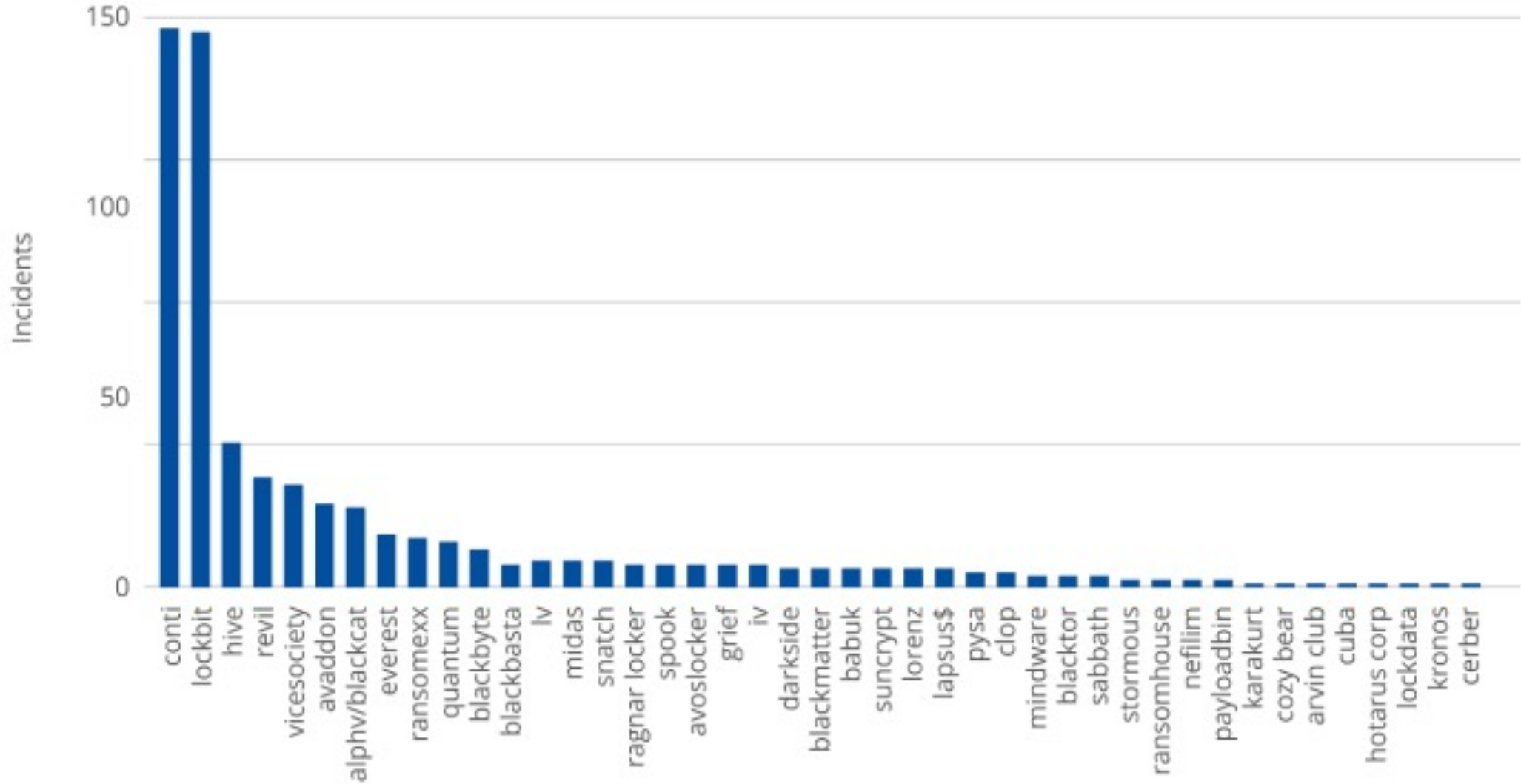


- A zsarolóvírus incidensek számának összehasonlítása az egyes ágazatokban





Zsarolóvírus incidensek analízise





Ajánlások



- Ellenőrzött, naprakész **biztonsági mentés** ami a hálózattól el van szigetelve
- Alkalmazza a **biztonsági mentés 3-2-1** szabályát.
- A **személyes adatokat** a GDPR rendelkezéseinek megfelelően **titkosítva tárolja**, és használja a megfelelő kockázatalapú ellenőrzéseket
- **Biztonsági szoftver** futtatás
- **Biztonságtudatosság** naprakészen tartása
- Kockázatértékelések
- Rendszergazdai jogok korlátozása



Megelőzés



- Csak ellenőrzött forrásból telepítsünk
- Ismeretlen feladótól származó e-maileket ne nyissunk meg
- Biztonsági mentés készítés hetente, naponta



Reagálás zsarolóvírusokra



- Forduljon a Nemzeti Kibervédelmi Intézethez
- Ne fizessen váltságdíjat
- Az érintett rendszereket helyezze karanténba
- Később még lehet feloldása a zsarolásnak



NO MORE RANSOM



NEMZETI KIBERVÉDELMI INTÉZET



Köszönöm a figyelmet!

csirt@nki.gov.hu

Kibertámadás! Podcast

nki.gov.hu